

The General Data Protection Regulation

Compliance monitoring by the CNPD

19th October 2017

Esch-sur-Alzette (Belval)



Christophe Buschmann

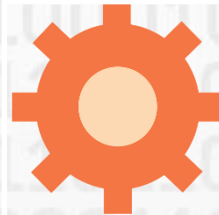
Commissioner

Agenda



Tasks and powers
of the DPA

Approach



Investigation -key
steps

Practical
recommendations



Tasks and powers of the DPA





Paradigm shift

No mandatory regular reporting towards CNPD

Notification /
authorization

Compliance
audit

But: The accountability principle requires documentation and internal reporting





Tasks and powers of the DPA

Article 57 Tasks: Each supervisory authority shall on its territory:

- **monitor and enforce** the application of this Regulation
- **conduct investigations** on the application of this Regulation, including on the basis of information received from another supervisory authority or other public authority;
- **monitor relevant developments**, insofar as they have an impact on the protection of personal data, **in particular the development of information and communication technologies and commercial practices**;
- ...

Article 58 Powers: Each supervisory authority shall have all of the following investigative powers:

- to carry out **investigations in the form of data protection audits**;
- to obtain, from the controller and the processor, **access to all personal data and to all information necessary** for the performance of its tasks;
- to obtain **access to any premises of the controller and the processor**, including to any data processing equipment and means, in accordance with Union or Member State procedural law.
- ...

Approach



CNPD

COMMISSION
NATIONALE
POUR LA
PROTECTION
DES DONNÉES



Controls and its objectives

Identify
recurring and
specific
problems

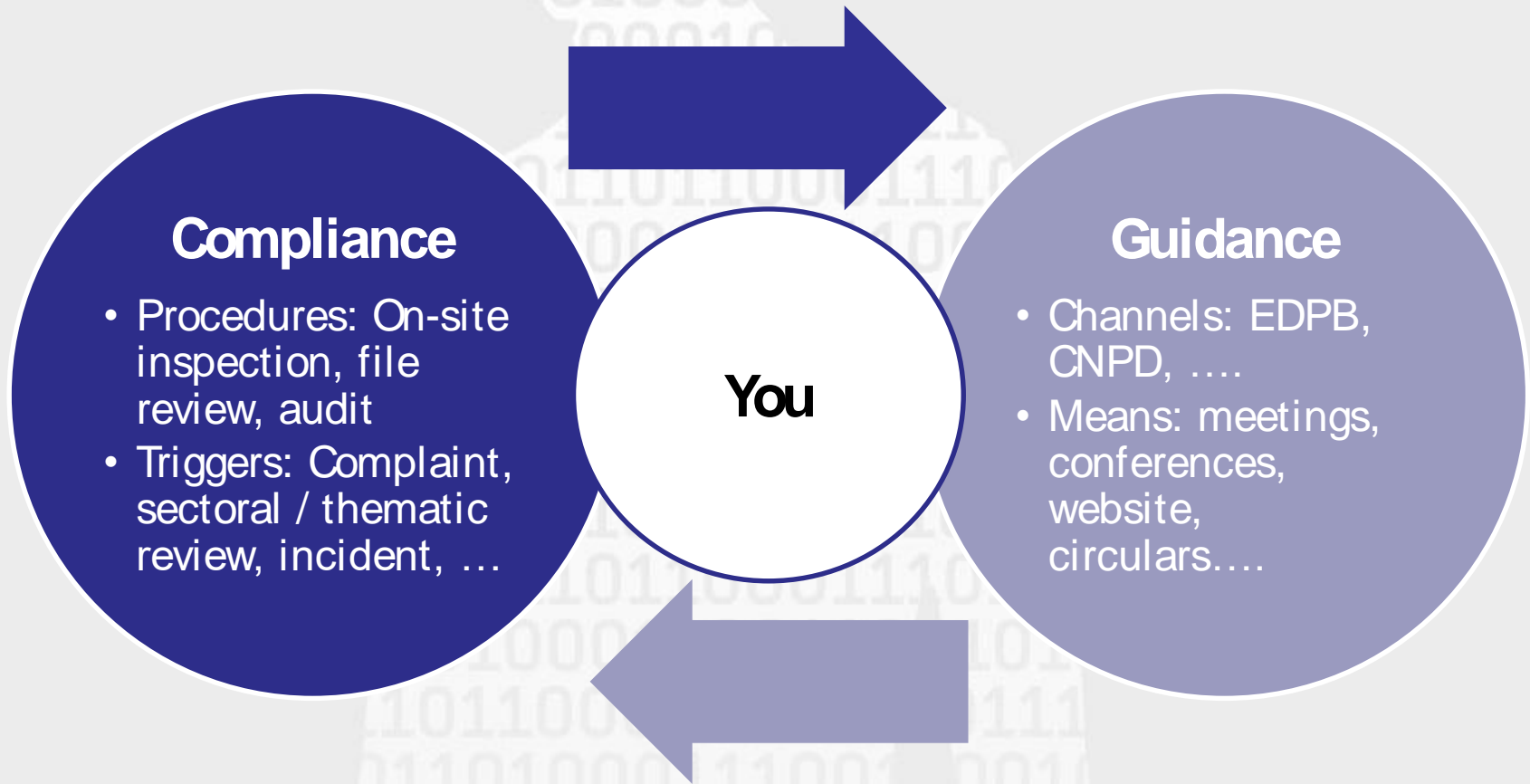
Check upon
correct
implementation
of guidance

Investigate in
case of reported
problems

Verify the
implementation
of action /
mitigation plans



The right balance



Compliance

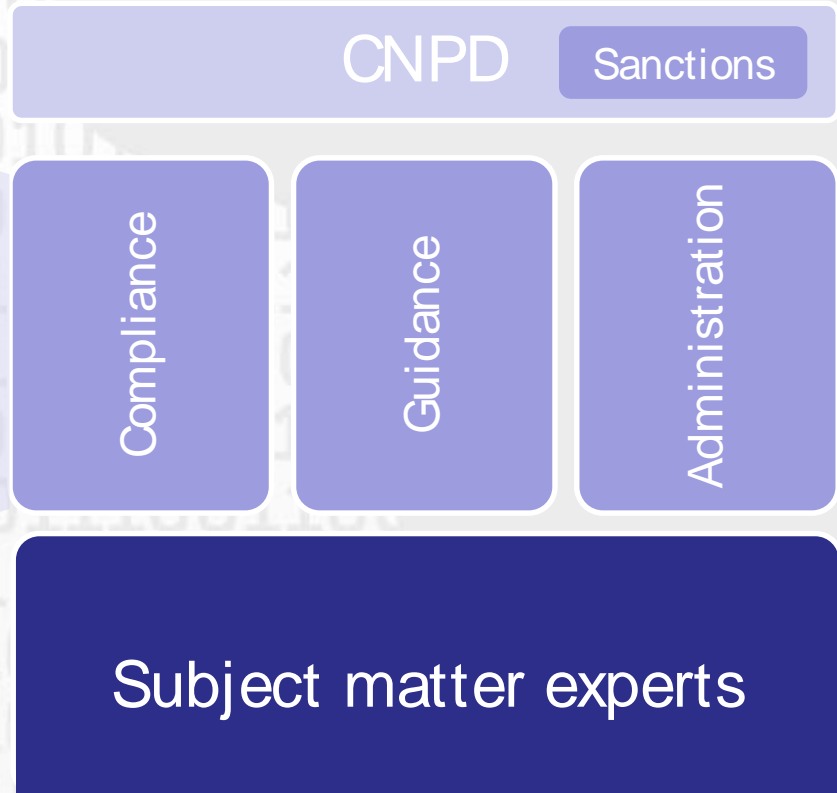
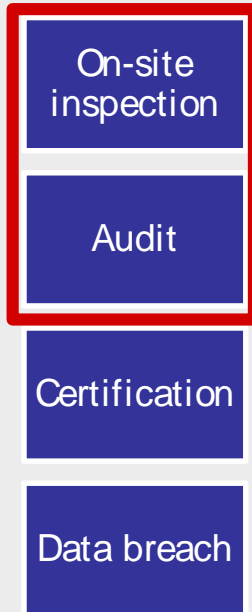
- Procedures: On-site inspection, file review, audit
- Triggers: Complaint, sectoral / thematic review, incident, ...

You

Guidance

- Channels: EDPB, CNPD,
- Means: meetings, conferences, website, circulars....

Organizational setup



Stakeholders



Commissioners



Head of investigation



Investigator



Expert



European cooperation



Types de contrôle

On-site inspection

- Inspection at the premises of the controller / processor
- Specific/limited scope
- One-off visit – where applicable triggers a file review

File review

- Questionnaire including a document request
- Review of answers and other relevant documents
- Switch to on-site inspection or data protection audit according to preliminary results

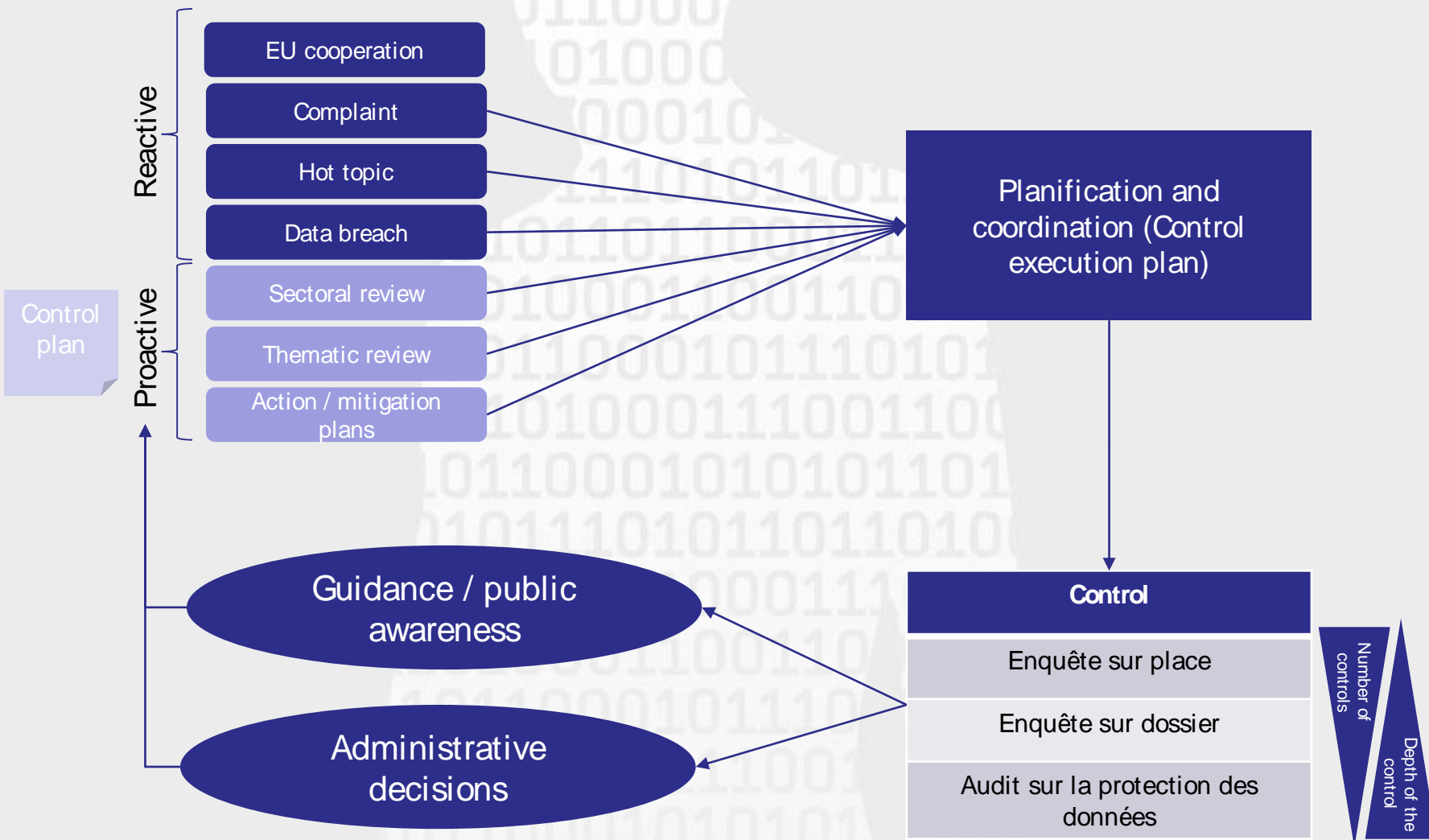
Data protection audit

- In depth review – broader in scope
- Multiple exchanges in form of meetings and off-site communication to exchange information and documents
- Risk based adaptation – refinement of scope during audit execution

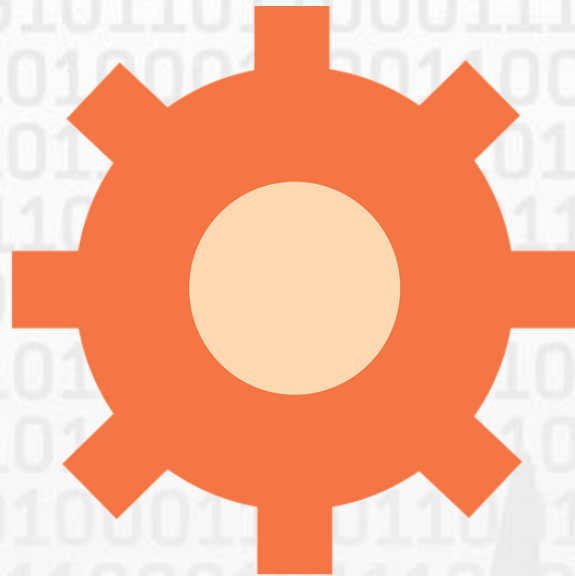




Control framework



Control - key steps





Control - Key steps

One-site support: Operation of IT systems to be done by your staff. Access to facilities with your presence.

Independence: Head of investigation not allowed to vote

Prior notice: In general, on-site inspections are not announced upfront. Data protection audits will be announced.

One-site presentation: Identification with a dedicated badge. Possibility to obtain confirmation upon contacting CNPD.

Discretion: Minimizing the impact on your business

Formalism: Administrative decision - not necessarily a sanction



Framework: Transparent and structured approach

Documentation: If applicable, a list of documents to be prepared will be provided – it may also include other organisational elements

Formalism: Minutes of the control, and if necessary an audit report – possible via encrypted email

Interactions: Possibility of hearing and / or other (formal) exchanges

Reply: Communicated in a clear way - aligned on a case by case basis - prevent problems (no response)

Recommendations / formal notice: No administrative decision - clarification of our expectations

Appeals: Time-limits apply

Practical recommendations





Before the control

Inform your staff of the possibility of a control/investigation

Define upfront an internal point of contact - check his availabilities

Inform yourself on where to find relevant data protection documentation – if applicable together with relevant personnel

If applicable involve the DPO in the setup of internal procedures

Involve relevant personnel since the beginning (in particular for on-site inspections and data protection audits)

Avoid problems in the first place: Complaints, data breaches, lack of follow up on mitigation plans,...



During the control

**Be transparent
cooperative and
honest**

**Check quality and
completeness of
documents and other
elements that you
provide us**

**Be specific in yours
answers – avoid
potential
misunderstandings**

**If applicable – make
sure relevant experts
are available (e.g. IT)**

**Keep up mutual
respect -
professionalism and
politeness**

**Be proactive in case
relevant elements
have not requested
explicitly**

**Don't hesitate to ask
questions**



After the control

Check the minutes and provide us your comments

Respect the deadlines

Stay available and reachable for questions

Take into account recommendations and notices

Inform us about measures already taken or that you plan to take – including a formal commitment and deadlines

Check completeness and accuracy of documents and other elements that you have provided us (in particular if a document request has been provided upfront)

Don't hesitate to contact us for any questions

You have to right for a hearing – avoid possible misunderstandings



After the decision

Review the decision – a decision does not always include a sanction

Be conscious about time-limits that apply for appeals

Don't hesitate to contact us for any question or comment

Respect the potential commitment that you engaged for (e.g. implementation of mitigation plans)

If applicable – check witch actions you need to take (e.g. stop or change certain processing activities)

If applicable – communicate with us if it in case it is impossible for you to implement the decision